Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.789

ID 기반 서명 기법을 이용한 IP 카메라 인증 및 키 교환 프로토콜*

박 진 영,† 송 치 호, 김 숙 영, 박 주 현, 박 종 환‡
상명대학교

IP Camera Authentication and Key Exchange Protocol Using ID-Based Signature Scheme*

Jin Young Park,† Chi-ho Song, Suk-young Kim,
Ju-hyun Park, Jong Hwan Park‡
Sangmyung University

요 약

현재 광범위하게 사용되는 IP 카메라는 모바일 기기를 통해 원격으로 IP 카메라를 제어하는 기능을 제공한다. 이를 위해 카메라 제조사가 지정한 웹사이트에서 IP 카메라 소프트웨어를 설치하고, IP 카메라와 모바일 기기 간 패스워드를 통해 인증을 거치게 된다. 그러나 현재 사용되는 많은 제품은 IP 카메라와 모바일 기기 간 보안채널을 제공하지 않아서 그 두 주체 간 전송되는 모든 ID 및 패스워드가 그대로 노출되는 문제가 있다. 이러한 문제점을 해결하기 위해 본 논문에서는 ID 기반 서명기법을 이용한 상호 인증 및 키 교환 프로토콜을 제안한다. 제시된 프로토콜의 특징은 (1) ID 기반 서명과 함께 IP 카메라에 내장된 ID 및 패스워드를 이용하여 상호인증을 수행하고, (2) 프로토콜 메시지 전송과정에서 IP 카메라를 특정할 수 있는 ID 및 패스워드가 노출되지 않으며, (3) 디피-헬만 키 교환을 사용하여 전방향 안정성을 제공하고, (4) 외부 공격자뿐만 아니라 ID-기반 서명의 마스터 비밀키를 가지고 호기심을 가진(honest-but-curious) 제조사에 대해서도 안전성을 가진다.

ABSTRACT

Currently widely used IP cameras provide the ability to control IP cameras remotely via mobile devices. To do so, the IP camera software is installed on the website specified by the camera manufacturer, and authentication is performed through the password between the IP camera and the mobile device. However, many products currently used do not provide a secure channel between the IP camera and the mobile device, so that all IDs and passwords transmitted between the two parties are exposed. To solve these problems, we propose an authentication and key exchange protocol using ID-based signature scheme. The proposed protocol is characterized in that (1) mutual authentication is performed using ID and password built in IP camera together with ID-based signature, (2) ID and password capable of specifying IP camera are not exposed, (3) provide forward-secrecy using Diffie-Hellman key exchange, and (4) provide security against external attacks as well as an honest-but-curious manufacturer with the master secret key of the ID-based signature.

Keywords: IP camera security, ID-based signature, password authentication

Received(03. 26. 2018), Modified(07. 10. 2018), Accepted(07. 30. 2018)
* 본 연구는 2017년도 상명대학교 교내연구비를 지원받아 수행하였음.
† 주저자, jinjin401@naver.com
‡ 교신저자, jhpark@smu.ac.kr (Corresponding author)

I. 서 론

IP 카메라는 사용자가 원하는 장소에서 실시간으로 발생하는 상황을 파악하기 위한 수단으로 광범위하게 사용되고 있다. IP 카메라를 제어하기 위해 흔히 사용자는 모바일 기기를 활용하는데, 이 경우 사용자는 언제 어디서든 원격으로 IP 카메라를 제어하는 것이 가능하다. 모바일 기기는 카메라 제조사가 지정한 웹사이트에서 IP 카메라 소프트웨어를 다운로드 받아 설치하고, IP 카메라와 모바일 기기 간 인증을 수행한다. 대부분 IP 카메라의 인증에 사용되는 ID 및 패스워드를 소프트웨어에 다시 입력하여 두 주체 간 인증을 수행한다[1]. 안전성 강화를 위해 사용자는 제조사에 의해 초기 설정된 패스워드를 새로운 것으로 변경할 수 있는데, 이러한 패스워드 변경이 성공적으로 이루어지면 IP 카메라는 사용자만이 제어할 수 있는 상태가 된다.

그러나 현실적으로 IP 카메라를 해킹하고 사용자의 사생활을 침해하는 사고는 증가하고 있다[2][3]. 악의적인 공격자가 초기에 설정된 또는 나중에 변경된 패스워드를 탈취하고, 이를 통해 IP 카메라와 정상적인 인증과정을 거친 후 IP 카메라를 제어하는 것이 가능하다. 이러한 공격이 가능한 이유는 IP 카메라와 모바일 기기 간 인증과정에서 ID 및 패스워드가 평문 형태로 노출되기 때문이다. 즉, 두 주체 간에 기본적인 보안채널조차 형성되지 않은 채 패스워드가 전송되는 경우가 많다. 실제 네트워크 분석 프로그램을 통해 두 주체 간 인증 시 전송되는 메시지를 분석하면, 사용자가 입력하는 IP 카메라의 ID 및 패스워드가 패킷의 헤더파일에 그대로 보이는 것을 확인할 수 있다. 또한 패스워드를 변경하는 과정에서도 새로운 패스워드가 그대로 노출되는 것을 볼 수 있다. 따라서 보안채널이 형성되지 않는 한, 아무리 패스워드를 변경하더라고 공격 대상이 되는 IP 카메라의 취약점은 그대로 유지된다.

이러한 문제점을 해결하기 위해 공개키 기반의 인증서(Certificate)를 사용하는 것이 고려될 수 있다. 이 방식에서는 IP 카메라 제조사가 먼저 신뢰된 루트 CA(Certificate Authority)로부터 자신의 인증서를 받은 후, 제조사가 중간 인증서 발급 기관이 되어 각 IP 카메라 제품마다 새로운 인증서를 탑재하는 방식이다. 이 경우 IP 카메라의 인증서는 3단 인증경로를 갖는 체인형태가 되고, 사용자는 IP 카메라와 인증 시 세 개의 체인 인증서를 모두 검증해야 한다. 그러나 인증서 방식은 제조사가 호기심을 갖고(honest-but-curious) 공격자로 되는 환경에서는 전혀 동작하지 않는다. 먼저 암호기법에 대한 인증서일 경우에는 보안 채널을 형성하기 위해 사용자가 IP 카메라의 인증서를 받으면, 세션키를 암호화하는 키 전달(key transport) 방식이 사용된다. 그러나 전송되는 인증서를 통해 제조사는 IP 카메라를 특정할 수 있다. 물론 공개키 인증서의 복호화 키를 알 수 있으므로 쉽게 암호화된 세션키를 복구할 수도 있다. 이 문제는 사용자가 초기 패스워드를 변경하는 과정에서도 그대로 유지된다. 이와 반대로 서명기법에 대한 인증서일 경우에는 디피-헬만 방식으로 세션키를 생성하는 것이 필요한 데, 이 경우 역시 인증서를 통해 제조사가 IP 카메라를 특정하는 것이 가능하다. 이론적으로는 IP 카메라와 사용자 사이에서 제조사가 중간자 공격을 하는 것도 가능하고, 만일 해당 IP 카메라의 사용자가 초기 패스워드를 변경하지 않은 경우라면, 제조사는 (서명키 인증서를 통해) 공격대상으로 파악된 IP 카메라의 ID와 초기 패스워드를 이용해 해당 제품에 접근하는 것도 가능하다.

본 논문에서는 이와 같은 문제점을 해결하기 위해 IP 카메라 사용 환경에 적합한 새로운 인증 및 키 교환 프로토콜을 제시한다. 제안되는 프로토콜은 최근 [4]에서 제시된 ID-기반 인증 및 키 교환 프로토콜을 IP 카메라 환경에 맞도록 수정한 것이다. 새로운 프로토콜에서는 ID 기반 서명, 디피-헬만, 그리고 IP 카메라에 내장된 ID 및 패스워드를 이용하여 상호 인증 및 키 교환을 수행하도록 설계된다. 특히 상호 인증 과정에서 전송되는 메시지에는 IP 카메라를 특정할 수 있는 어떠한 ID 및 패스워드도 포함되지 않고, 이로 인해 외부 공격자 및 호기심을 갖는 제조사가 해당 제품을 특정하는 것이 어렵다. 또한 전방향 안전성(forward secrecy)[5]을 보장하는 키 교환 프로토콜로 IP 카메라와 사용자의 서명키가 노출되어도 이전에 설립된 세션키는 알 수 없다. 마지막으로 (ID, 패스워드)에 대한 온라인 전수조사 공격을 완화하도록 IP 카메라 내부가 설계되었다면, 외부 공격자 및 호기심을 갖는 제조사가 (ID, 패스워드)를 추측하는 것도 어렵다. 제안되는 프로토콜은 인증 및 키 교환 프로토콜의 안전성 모델을 ID 기반 [6]에 맞도록 변형한 후, 그 안전성을 증명한다.

II. 현행 IP 카메라 동작 프로토콜

현재 유통되는 IP 카메라의 동작 프로토콜은 〔그림 1〕과 같다. 제조사는 각각의 IP 카메라에 대응하는 제품 고유의 패스워드 및 ID를 할당한다. 여기서 IP 카메라 구매자(이하에서는 사용자)는 고유 패스워드 및 ID를 제품 구매 시 알 수 있다고 가정한다.

1. IP 카메라는 기본적인 네트워크 통신 기능이 탑재된 채 제조되고, 사용자는 이를 구매한 후 필요한 곳에 설치를 시작한다.

2. 사용자는 IP 카메라 제조사가 지원하는 애플리케이션 스토어에서 구매한 제품을 제어할 수 있는 프로그램을 사용자의 모바일 기기에 설치한다.

3. 사용자는 IP 카메라 고유의 패스워드 및 ID를 입력하여 IP 카메라에게 사용자를 인증한다. 인증이 완료되면, 사용자는 이제부터 IP 카메라를 모바일 기기를 이용하여 제어한다.

4. IP 카메라 제조시 설정된 패스워드를 변경하려면, 사용자는 IP 카메라 제어 메시지를 통해 패스워드를 새롭게 변경한다.

위 프로토콜의 문제점은 사용자와 IP 카메라가 통신하는 채널이 기본적인 TCP/IP 기반 네트워크 통신이고 어떠한 보안채널도 수립되지 않는다는 것이다. 따라서 두 주체 간 통신되는 모든 메시지는 평문 형태로 노출된다. 실제로 네트워크 분석 프로그램을 통해서 전송되는 패킷을 살펴보면, 사용자가 입력한 패스워드 및 ID 정보가 그대로 노출되는 것을 확인할 수 있다. 심지어 사용자가 초기 패스워드를 수정하더라도 갱신된 패스워드마저 그대로 노출된다. 이는 악의적인 공격자가 언제든지 공격대상이 되는 IP 카메라에 접근하여 쉽게 제어할 수 있다는 것을 의미한다.

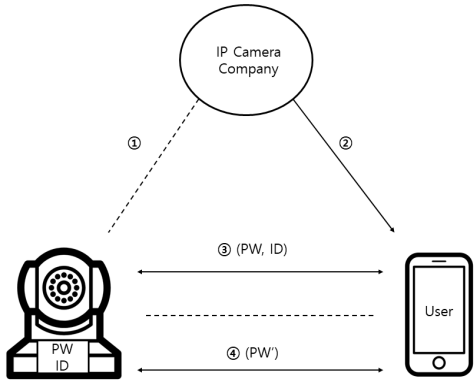

Fig. 1. IP camera operation protocol

III. 배경 지식

3.1 ID 기반 서명(IBS)

ID 기반 서명(IBS: ID-Based Signature) 기법은 네 개의 알고리즘 (Setup, KeyGen, Sign, Verify) 알고리즘으로 구성된다.

- Setup(1^{λ}) → (PP, msk): 보안상수 1^{λ}를 입력받고 시스템 전체에 사용되는 공개 파라미터 PP(Public Parameter)와 마스터키 msk(master secret-key)를 출력한다.
- KeyGen(ID, msk) → sk_{ID}: 마스터키 msk와 사용자의 ID를 입력받아서 사용자의 서명키 sk_{ID}를 출력한다.
- Sign(m, sk_{ID}) → σ: 메시지 m, 사용자 서명키 sk_{ID} 및 공개 파라미터 PP를 입력받아서 서명 σ를 출력한다.
- Verify(σ, m, ID, PP) → T/F: 검증 알고리즘은 서명 σ, 메시지 m, 사용자 ID 및 공개 파라미터 PP를 입력받아서 T(True) 또는 F(False)를 출력한다.

정확성(Correctness). 임의의 보안 상수 1^{λ}를 입력으로 하여 Setup으로부터 생성된 (PP, msk), 마스터키 msk와 사용자 ID를 입력받아 KeyGen으로부터 생성된 sk_{ID}에 대하여, 다음 검증식을 만족한다.

Verify(Sign(m, sk_{ID}), m, ID, PP)=T

안전성(Security). IBS 기법의 공격자는 임의의 ID를 선택하여 그에 대응하는 서명키 sk_{ID}를 받는다. 또한 임의의 사용자 ID와 메시지 m을 선택하여 서명 σ를 받는다. 이러한 질의는 다항식으로 표현되는 횟수만큼 시행될 수 있다. 질의 후 공격자는 자신이 질의하지 않은 사용자의 ID^{*}, 메시지 m^{*}에 대해서 서명 σ^{*}를 출력한다. 만일 서명 σ^{*}가

검증식을 통과하면 공격자는 공격을 성공한 것으로 본다. 일반적으로 IBS 기법에 대한 임의의 다항식 시간 공격자 A에 대하여 공격자의 성공확률이 무시할 만큼(negligible) 작다면, IBS 기법은 선택 메시지 공격(chosen message attack)에 대하여 안전하다고 한다.

3.2 유사 난수 함수(PRF)

유사 난수 함수(Pseudorandom Function)는 두 개의 값 $(K, x) \in \{0,1\}^{l_k} \times \{0,1\}^{l_i}$을 입력받아서 $f(K, x) \in \{0,1\}^{l_o}$을 출력하는 함수이다. PRF의 안전성은 키 공간 $\{0,1\}^{l_k}$에서 임의로 선택된 키 K에서 대해 정의된 $f_K(\bullet)$가 동일한 정의역과 공역에서 정의된 랜덤함수 $R(\bullet)$와 구별하는 것이 어렵다는 것으로 정의된다.

$f: \{0,1\}^{l_k} \times \{0,1\}^{l_i} \rightarrow \{0,1\}^{l_o}$이 PRF라 하는 것은, 다항식 시간 공격자 D에게 다음을 구별한 확률이 무시할 만한(negligible) 것으로 정의된다.

$$\left|\Pr[D^{f_k(\bullet)} = 1] - \Pr[D^{R(\bullet)} = 1]\right| \leq g(\lambda)$$

여기서 D에게는 f_K와 R중 임의로 선택된 함수에 접근할 수 있는 오라클이 주어진다. 그리고 g는 보안 상수 1^{λ}에 대하여 무시할 만할 값을 가지는 함수이다.

3.3 ID 기반 인증 및 키 교환 프로토콜 안전성

먼저 각 사용자들은 자신의 ID에 대응하는 비밀키 SK_{ID}를 받는다. 본 논문에서는 IBS를 기반으로 설계하므로 SK_{ID}를 서명키로 한다. 다음 인증 및 키 교환 프로토콜 단계에서는 통신 개시자(initiator)가 도전값(challenge)를 상대방(responder)에게 보내면, 이에 대한 응답값(response) 및 도전값을 보낸다. 마지막으로 개시자는 응답값을 보내서 프로토콜을 완료한다. 여기서 응답값은 IBS의 서명값이 된다. 이 과정을 거치면, 두 사용자는 서명 검증을 통해 상호 인증하고 공통의 세션키를 공유하게 된다.

안전성 모델은 Canetti-Krawczyk (CK) 모델[6]을 ID 기반으로 확장한 ID-CK 모델[7]을 고려한다. 이 모델에서는 교환된 세션키가 랜덤한 값과 구별하는 것이 어렵다는 것을 증명한다. 공격자 A에게는 다음과 같은 질의가 허용된다.

- Send(ID_i, ID_j): (ID_i, ID_j)를 지정하여 프로토콜 과정에서 원하는 메시지를 보내도록 한다.
- Corrupt(ID): ID에 대응하는 서명키 SK_{ID}를 받는다. 전방향 안전성을 위해 Test 세션에서 세션키가 설립된 이후에는 공격대상에 대한 서명키로 허용한다.
- SessionKeyReveal(ID_i, ID_j):(ID_i, ID_j)에 의해 완료된 프로토콜에서 공유된 세션키를 요청한다.
- StateReveal(ID_i, ID_j): (ID_i, ID_j)의 프로토콜 수행과정에서 사용된 state 정보를 요청한다.
- Test(ID_i, ID_j): 공격대상으로 (ID_i, ID_j)와 두 사용자가 수행한 프로토콜 중 세션 state[1]와 서명키가 질의되지 않는 세션을 선택한다.

공격자가 Test 대상으로 선택한 세션키에 대해 랜덤한 비트 $b \in \{0,1\}$을 선택해서, $b=1$이면 실제 세션키를 공격자에게 주고, $b=0$이면 랜덤하게 선택된 세션키를 준다. 이에 대해 공격자는 b'비트를 출력한다. 이 게임에서 공격자의 공격 성공 이익(advantage)는 공격자가 맞출 확률 $\Pr[b=b']$에 대해서 $|\Pr[b=b'] - 1/2|$로 정의된다.

정의 1. 위 게임에서 다항식 시간 공격자의 공격이익이 무시할 만하다면, ID 기반 인증 및 키 교환 프로토콜은 전방향 안전성 및 사용자 인증을 제공한다고 한다.

본 논문에서는 위 공격모델을 기반으로 두 사용자는 공격자에게 노출되지 않는 (ID, 패스워드)를 공유했다고 가정한다. 이 경우 공격자는 (1) 외부 공격자 및 (2) 마스터키를 가진 공격자로 구분한다. 다시 외부 공격자는 (a) 서명키를 갖지 않는 공격자 및 (b) 서명키를 갖은 공격자로 구분하고, 마스터키를 가진 공격자는 (c) 세션을 시작하지 않는 호기심을 가진(honest-but-curious) 공격자 및 (d) 세션을 시작하는 호기심을 가진 공격자로 구분한다.

1) 본 논문에서는 Test 세션에 대한 state 질의는 허용하지 않는다. 이것은 ID-CK 모델보다 약화된 것인데, 그 이유는 제안 프로토콜이 일회용 디피-헬만 키 교환을 바탕으로 세션키를 수립하는 과정에서 두 사용자의 세션 state 중 하나라도 노출되면 (ID, 패스워드)의 전수조사로 익명성이 깨질 위험이 있기 때문이다.

(a)와 (b)는 일반적인 외부의 공격자를 가정하고, (c)와 (d)는 제조사를 공격자로 가정한 것이다. 자연스럽게 (c)와 (d) 공격자에게는 Corrupt 질의는 무의미하므로 제거된다. 본 논문에서는 제조단계에서부터 악의적인(malicious) 공격자는 고려하지 않는다. 악의적인 제조사라면, 난수발생기를 위조하거나 시스템에 침투할 수 있는 백도어(backdoor)를 만드는 것도 가능하므로 그러한 공격까지 고려한 안전성 모델 설정은 쉽지 않기 때문이다.

3.4 암호학적 가정들

RSA 키 생성 알고리즘 $\mathrm{KG}_{\mathrm{RSA}}(1^{\lambda})$는 보안 상수(security parameter) 1^{λ}을 입력으로 하여 서로 다른 두 소수 p, q를 선택하고, $N=pq$에 대한 $ed \equiv 1 \pmod{\phi(N)}$ 을 만족하는 e, d를 계산하여 RSA 파라미터 (N, p, q, e, d)로 출력한다. 여기서 N은 $-1 \notin QR_N$인 Blum 정수라고 하자. 즉, p와 q 모두 4로 나눈 나머지가 3이 되도록 선택한다. 그리고 서로 다른 소수 p_1, q_1에 대해서 $p=2p_1+1$, $q=2q_1+1$인 소수를 생성한다.

그룹 위수가 숨겨진 강한 디피-헬만 가정.[8] $\mathrm{KG}_{\mathrm{RSA}}(1^{\lambda})$로 RSA 파라미터 (N, p, q, e, d)를 구하면, 여기서 부호화된(signed) QR 그룹[2][8](이하에서는 QR_N^+으로 표기한다.)의 생성원 하나를 랜덤하게 선택한다. 이를 $g \in QR_N^+$ 라 하자. 여기서 g의 위수는 p_1q_1임을 상기하자. 또한 QR_N^+에서 랜덤하게 두 개의 $g^a, g^b \in QR_N^+$를 택한 후 공격자에게 (N, g, g^a, g^b, O)를 준다. 여기서 오라클 O는 입력값 (g, g_1, g_2, g_3)를 받으면, $g_3 = g_1^{Dlog_g g_2}$인지를 결정해준다. 즉, g_3가 g_1과 g_2의 디피-헬만 값이면 1을 주고, 아니면 0을 주는 오라클이다. [8]에서는 소인수분해 문제가 이 가정의 문제로 환원됨을 보였다.

그룹 위수가 알려진 강한 디피-헬만 가정. 위 가정과 동일하게 RSA 파라미터 (N, p, q, e, d)에서 QR_N^+의 생성원 $g \in QR_N^+$ 를 생성하고, 두 개의 랜덤 $g^a, g^b \in QR_N^+$를 택한다. 그리고 QR_N^+의 그룹 위수 p_1q_1을 포함해서 $(N, p_1q_1, g, g^a, g^b, O)$를 준다. 여기서 오라클 O는 위와 같다. 이 문제는 그룹 위수를 알려주는 기존의 강한 디피-헬만 가정[9]과 유사하게 볼 수 있다. 차이점은 N대신에 비슷한 사이즈를 갖는 소수로 바뀐 것과 그룹 위수가 p_1q_1대신에 훨씬 더 작은 소수[3]이다.

IV. IP 카메라 인증 및 키 교환 프로토콜

4.1 GQ-IBS 기법

IP 카메라 보안 프로토콜을 제안하기 전에 기존 Guillou-Quisquater IBS [10]를 기술한다.

- **Setup(1^{λ}):** $\mathrm{KG}_{\mathrm{RSA}}(1^{\lambda})$ 알고리즘으로부터 RSA 파라미터 (N, p, q, e, d)를 생성한다. p와 q는 소수 p_1과 q_1에 대해 $p=2p_1+1$와 $q=2q_1+1$의 형태로 생성한다. 해쉬함수 $H_1 : \{0,1\}^* \rightarrow QR_N$ 및 $h_1 : \{0,1\}^* \rightarrow \{0,1\}^l$를 정의한다. 공개 파라미터 $\mathrm{pp}=(N, e, H_1, h_1)$와 마스터키 $\mathrm{msk}=(N, d)$를 출력한다.
- **KeyGen(ID, msk, PP):** 사용자 ID에 대응하는 서명키 $sk_{ID} = H_1(ID)^d \pmod{N}$ 을 생성한다.
- **Sign(m, sk_{ID}, PP):** 랜덤하게 $g \in Z_N^*$을 생성한다. $y = g^e \pmod{N}$ 을 계산한 후, $c \leftarrow h_1(y, m)$ 을 계산한다. 그리고 $z \leftarrow sk_{ID}^c \cdot g \pmod{N}$ 을 계산하고 서명 $\sigma = (z, y)$를 출력한다.
- **Verify(σ, m, ID, PP):** $\sigma = (z, y)$라 하자.
  1. $c \leftarrow h_1(y, m)$을 계산한다.
  2. $A \leftarrow z^e \cdot H_1(ID)^{-c} \pmod{N}$ 을 계산한다.
  3. 등식 $y = A$을 확인한다. 같으면 T를 출력하고, 다르면 F를 출력한다.

GQ-IBS 기법에서는 서명을 할 때마다 Z_N^*에서 랜덤한 값 g를 생성한다. 반면 [4]에서 제시한 IBS

2) Z_N^*의 원소를 $\{-(N-1)/2, \ldots, (N-1)/2\}$로 표현할 때, QR_N의 원소 각각에 절대값을 취해서 얻어지는 그룹을 QR_N^+라 한다. 제안된 프로토콜에서는 변형된 GQ-IBS의 파라미터와는 독립적으로 $g \in QR_N^+$에 대응하는 연산에 대해서만 QR_N^+ 그룹의 연산을 적용한다.

3) 보통 정수 기반에서는 보안 상수 λ에 대해 2λ 사이즈를 갖는 위수를 설정한다. 여기서는 N이 강한 소수의 곱이므로 거의 $N \approx p_1q_1$ 사이즈인 위수를 갖는다.

는 변형된 GQ-IBS로 볼 수 있는데, 공개 파라미터에 g를 추가하여 매 서명마다 동일한 g를 사용한다. 그 결과 [4]에서는 동일한 g를 사용함으로써 새로운 디피-헬만 파라미터를 공유할 필요 없이 서명값만 교환함으로써 g를 이용한 디피-헬만 키 교환이 가능한 장점을 가진다. 계산량 측면에서는 서명 생성 과정에서 GQ-IBS가 [4]의 변형된 IBS보다 더 효율적인 계산이 가능하고, 공개 파라미터의 길이도 짧아진다.

그러나 본 논문에서는 안전성 증명을 위해 모듈러스 N에서 새로운 그룹(다음 절에서 설명되는 QR_N^+)을 설정하고, 그 그룹에서 디피-헬만 키 교환을 수행하는 과정이 필요하다. 따라서 새롭게 제안하는 인증 및 키 교환 프로토콜에 맞추어 본 논문에서는 GQ-IBS를 사용한다. GQ-IBS 기법의 안전성은 RSA 가정 하에서 선택 메시지 공격에 안전하다는 것이 증명되었다. [10],[11].

IBS는 이산대수 문제로 안전성이 증명될 경우 타원곡선 암호로 구현되어 더 좋은 효율성을 가질 수 있다. 예를 들어, [11],[12]에서 제시한 IBS 기법들은 공개키 서명을 두 번 적용하는 설계원리를 통해 이산대수에 안전하도록 설계되었다. 그러나 그러한 기법들은 본 논문에서 제시하는 프로토콜에 적합하지 않다. 그 이유는 전자서명 인증서를 사용하는 방식처럼, IBS 서명 생성 시 각각의 ID에 대응되는 동일한 값을 매번 서명에 포함시키는 것이 필요하기 때문이다. 이렇게 변하지 않는 값은 여전히 제조사에게 ID를 특정하는 값으로 사용된다.

4.2 IBS 기반 인증 및 키 교환 프로토콜

[그림 2]에서는 IP 카메라 보안을 위해 앞 절의 GQ-IBS 기법을 이용하여 두 주체 간 인증 및 키 교환을 수행하는 프로토콜을 제안한다. 이를 위해 몇 가지 사항을 가정한다. (1) A를 IP 카메라라 하고 B는 그 카메라를 동작시키는 주체라 하자. (2) A와 B 모두 IBS 기법을 위해 공개 파라미터 pp가 탑재되어 있고, 각각 자신의 ID에 대응하는 서명키를 갖고 있다고 한다. (3) A에는 제조 시 내장된 ID_A 및 패스워드 pw가 있고, 제품을 구매하는 사용자가 이들을 인지할 수 있다고 하자. 이 경우 IP 카메라 A는 초기값으로 $(sk_A,\ ID_A,\ pw,\ pp)$이 탑재되고, 제품을 구매한 사용자의 기기 B는 자신의 ID_B에 대응하는 $(sk_B,\ pp)$를 애플리케이션 프로그램 설치 시 받는다. 이 과정을 보다 자세히 아래 a, b, c 단계로 설명한다.

a. 먼저 RSA 모듈러스 N을 구성하는 p와 q는 소수 p_1과 q_1에 대해 $p=2p_1+1$와 $q=2q_1+1$의 형태로 생성한다. 그리고 GQ-IBS를 위한 공개 파라미터 (N,e)와 마스터키 (N,d)를 생성한다.

또한 N은 $-1\notin QR_N$인 Blum 정수라고 하자. (즉, p와 q 모두 4로 나눈 나머지가 3이 되도록 선택한다.) 여기서 부호화된 QR 그룹 QR_N^+의 생성원을 랜덤하게 선택한다. 이를 $g\in QR_N^+$ 라 하자.

해쉬함수 $H_1:\{0,1\}^*\rightarrow QR_N,\ \ h_1:\{0,1\}^*\rightarrow\{0,1\}^l$와 함께 새로운 해쉬함수 $H_2:\{0,1\}^*\rightarrow\{0,1\}^{s+2t}$ 를 정의한다. (여기서 s,t는 보안상수 λ에 의해 결정된다.) 그리고 PRF $f:\{0,1\}^t\times\{0,1\}^*\rightarrow\{0,1\}^w$ 를 정의한다. (여기서도 w는 보안상수 λ에 의해 결정된다.) 최종적으로 $pp=(N,e,g,H_1,H_2,h_1,f)$이고, 마스터키는 $msk=(N,d)$이다.

b. IP 카메라 A는 ID_A에 대응하는 서명키로 $sk_A=H_1(ID_A)^d\ (\mathrm{mod}\ N)$를 받는다. 그리고 pw 및 ID_A가 내장된다.

c. 사용자 B는 pp와 함께 ID_B에 대응하는 서명키로 $sk_B=H_1(ID_B)^d\ (\mathrm{mod}\ N)$를 받는다.

이제 [그림 2]의 인증 및 키 교환 프로토콜을 단계적으로 설명한다.

1. A는 난수 $R_A\in Z_N$를 생성한다.

2. A는 $u_A=g^{R_A}\in QR_N^+$ 를 생성한다. u_A는 도전-응답 프로토콜의 도전값으로 B에게 전송된다.

3. B는 A로부터 ID_A및 pw를 입력한다.

4. B는 난수 $R_B\in Z_N$를 생성한다.

5. B는 $u_B=g^{R_B}\in QR_N^+$ 를 생성한다.

6. B는 $g_1\|K_1\|K_2=H_2(g^{R_A},g^{R_B},g^{R_AR_B})\in\{0,1\}^{s+2t}$를 생성한다. 여기서 g^{R_A}는 A에게 받

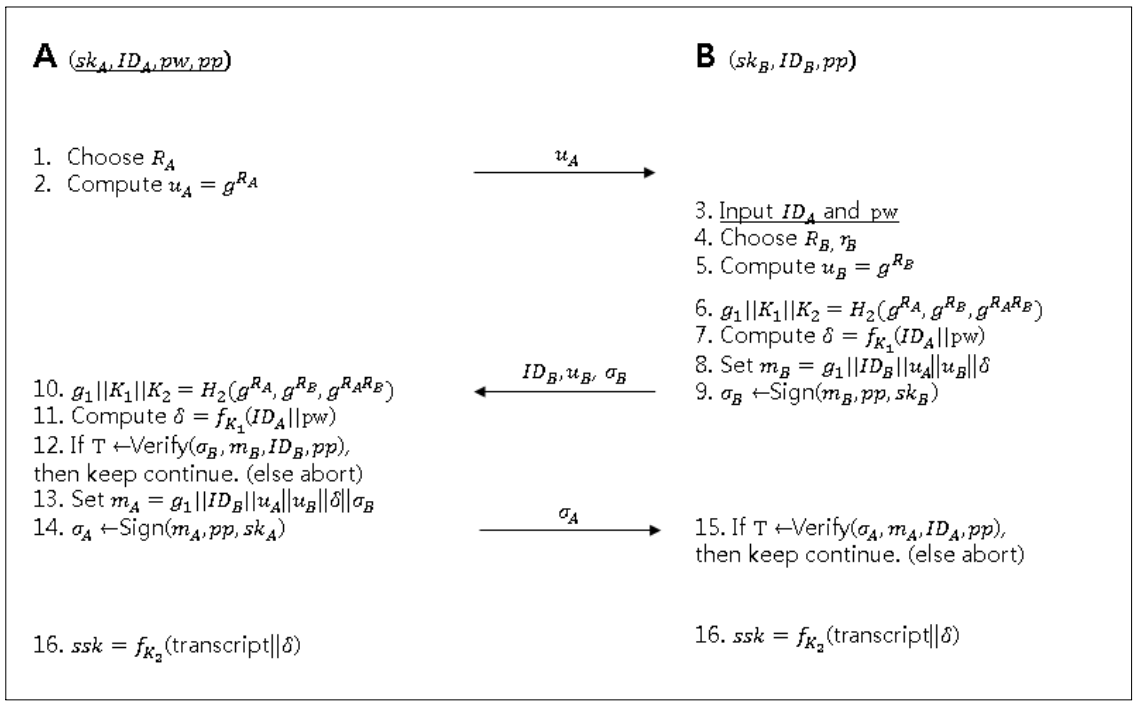

Fig. 2. New ID-based authentication and key exchange protocol

은 u_A값이고, $g^{R_A R_B}$는 $(u_A)^{R_B} \in QR_N^+$ 으로 계산된다.

7. B는 $\delta = f_{K_1}(ID_A||pw)$를 계산한다.

8. B는 $m_B = g_1||ID_B||u_A||u_B||\delta$를 생성한다.

9. B는 GQ-IBS 서명 알고리즘으로 m_B에 대한 서명 σ_B를 생성한다. 그 다음 (ID_B, u_B, σ_B)을 A에게 전송한다. 여기서 서명 σ_B는 도전-응답 프로토콜에서 도전값 u_A에 대한 B의 응답값이다.

10. A는 $g_1||K_1||K_2 = H_2(g^{R_A}, g^{R_B}, g^{R_A R_B}) \in \{0,1\}^{s+2t}$를 생성한다. 여기서 g^{R_B}는 B에게 받은 u_B값이고, $g^{R_A R_B}$는 $(u_B)^{R_A} \in QR_N^+$ 으로 계산된다.

11. A는 $\delta = f_{K_1}(ID_A||pw)$를 계산한다.

12. A는 m_B에 대한 서명 σ_B을 검증한다. 검증이 통과되지 않으면, 프로토콜을 중단하고, 검증이 통과되면 다음을 진행한다.

13. A는 $m_A = g_1||ID_B||u_A||u_B||\delta||\sigma_B$를 생성한다.

14. A는 GQ-IBS 서명 알고리즘을 이용하여 m_A에 대한 서명 σ_A를 생성한다. 그 다음 σ_A을 B에게 전송한다. 여기서 서명 σ_A는 도전-응답 프로토콜에서 도전값 u_B에 대한 A의 응답값이다.

15. B는 m_A에 대한 서명 σ_A을 검증한다. 검증이 통과되지 않으면, 프로토콜을 중단하고, 검증이 통과되면 다음을 진행한다.

16. A와 B는 K_2를 이용하여 프로토콜 수행 중에 주고받은 전송 데이터(transcript)와 δ를 PRF 입력으로 넣어 $ssk = f_K(transcript||\delta) \in \{0,1\}^w$를 구한다.

4.3 제안된 프로토콜의 특징

〔그림 2〕에서 제시된 프로토콜의 특징을 설명한다. 첫째, A에 대응되는 패스워드 pw 및 ID_A은 프로토콜의 전송메시지에서 노출되지 않는다. 심지어 ID_A마저 노출시키지 않는데, 이것은 실제 IP 카메라 제조사의 경우 ID_A에 대응하는 패스워드를 알 수 있기 때문이다. 만일 IP 카메라의 ID_A가 노출된다면 악의적인 제조사는 해당 제품에 내장된 패스워드를 이용하여 IP 카메라 사용자 B를 가장하는 공격이 가능하게 된다. 둘째, A에 대응되는 패스워드 pw 및 ID_A를 사용자인 B가 직접 입력함으로써, A로서는 사용자 B가 정상적으로 카메라를 구매하고 패스워드 및 ID_A를 입력했다는 것을 (서명 검증과 함께) 인증하게 된다. 이 과정은 특히 IP 카메라가 처음으로 통신을 개시할 때 중요한다. 그 이유는 A의 무선 네트워크 범위에 복수의 사용자 후보들이 있을 수 있는데, 이 경우 A는 패스워드 및 ID_A를 이용하여 복수의 사용자들 중 누구와 통신을 개시할지 결정할 수 있기 때문이다. 셋째, 제안된 프로토콜은 QR_N^+그룹에서 디피-헬만 키 교환을 수행함으로써 프로토콜 수행 시 생성된 난수 정보가 노출되지 않는 한 전방향 안전성(forward secrecy)을 보장한다. 즉, 세션키가 설립된 이후 각자의 서명키가 노출되어도 이전에 설립된 세션키는 안전하게 보호된다. 따라서 세션키가 설립된 이후 초기 패스워드를 새롭게 (그리고 패스워드 사전 공격에 견디도록) 바꾼다면, 그 이후 세션키가 노출되어도 전방향 안전성을 보장하는 채널에 의해 악의적인 제조사로부터도 안전한 패스워드가 된다.

공격자 관점에서의 특징: 이제 안전성 증명 이전에 공격자의 관점에서 프로토콜의 특징을 설명한다. 먼저 (서명키를 갖지 않은) 외부의 공격자 입장에서는 전송 메시지들을 관찰 한 후, A의 새로운 도전값 u_A에 대응하는 서명을 만들어야 한다. 서명위조는 공격자가 모르는 g_1, δ를 메시지에 포함하여 이루어져야 하는데, 특히 이 값들은 u_A와 u_B의 디피-헬만 값인 $g^{R_AR_B}$을 알아야 구할 수 있다. 또한 g_1, δ를 구해도 모르는 서명키에 대한 서명 위조를 해야 하므로, 이 경우는 자연스럽게 GQ-IBS의 안전성에 의해 방어된다.

또한 공격자가 B의 서명키를 가지고 공격하는 경우도 생각할 수 있다. 즉, B를 가장해서 통신을 시도할 수 있으나, 프로토콜이 정상적으로 완료되기 위해서는 A의 도전값 u_A에 대응하는 서명 σ_B을 공격자의 응답값으로 보내야 한다. 이 과정에서 g_1, K_1, K_2은 알 수 있으나, pw 및 ID_A를 모르기 때문에 온라인상에서 pw 및 ID_A를 시도하는 공격을 수행해야 한다. 이러한 온라인 공격은 pw 및 ID_A의 경우의 수만큼 인증 시도를 허용한다면 성공할 수도 있으나, 프로토콜의 12번 과정에서 A 내부에 온라인 공격에 대응하는 방법[4]을 설정하는 것으로 방어할 수 있다. 더구나 하나의 pw 및 ID_A에 대해 서명을 생성해야 하는데, GQ-IBS 서명 알고리즘에 의하면 최소 한 번의 지수승을 해야 한다.

다음으로 호기심을 갖는(honest-but-curious) 제조사가 공격하는 경우를 살펴본다. 먼저 마스터키를 가지고 있으나, B를 가장해서 세션을 시작하지는 않는 공격자를 고려한다. 공격자는 A가 생성한 서명 σ_A를 검증하는 과정을 통해 A의 pw 및 ID_A를 전수조사할 수 있다. 그러나 앞에서 설명한 외부 공격자처럼, u_A와 u_B의 디피-헬만 값인 $g^{R_AR_B}$을 알아야 구할 수 있는 g_1, K_1 (그러므로 δ)을 모르기 때문에 서명 검증을 통과하는 것이 어렵다. 주의할 점은 GQ-IBS의 서명이 $z \leftarrow sk_{ID}^c \cdot g \pmod N$와 $y = g^e \pmod N$으로 계산된 $\sigma = (z, y)$이 되어야 한다. 여기서 $c \leftarrow h_1(y, m)$로 계산된다. GQ-IBS 서명은 $\sigma = (z, c)$으로도 될 수 있는데, 중요한 점은 해쉬값 c가 서명 σ에 포함되면 안 된다는 것이다. 만일 $\sigma = (z, c)$라면, 공격자는 자신이 제조 당시 설정한 ID를 전수조사하는 방법으로, ID 하나에 대해 $z^e H_1(ID)^{-c} = g^e \pmod N$를 구한 후, 마스터키 또는 N의 소인수들을 통해 구할 수 있는 $e^{-1} = d$를 지수승하면 g를 구할 수 있다. 이 g값을 z에서 제거하면 sk_{ID}^c를 알고, c^{-1}를 지수승하면 sk_{ID}를 획득할 수 있다. 이 값이 $sk_{ID} = H_1(ID)^d$값과 일치한다면, 추측한 ID가 옳다는 것을 알 수 있다. 따라서

4) 한 예로 미리 정해진 인증횟수를 통과하지 못하면, 일정한 시간을 지연시킨 후 다시 인증을 시도하도록 하는 것이다.

다항식 시간의 전수조사로 안전성이 약화된다. 반대로 해쉬값 c가 서명 σ에 포함되지 않으면, 공격자는 $(g_1,\ \delta)$의 경우의 수만큼 또는 $(ID,\ c)$의 경우의 수만큼 전수조사를 해야 한다. 이러한 관찰은 서명이 $\sigma=(z,y)$ 또는 $\sigma=(z,c)$에 따라서 안전성이 달라질 수 있다는 것을 보여주는 사례이다.

다음으로 호기심을 갖는 제조사가 세션을 시작하면서 공격하는 경우이다. 이 경우는 앞서 본 외부 공격자처럼 온라인 공격을 통해 A의 도전값 u_A에 대응하는 서명 σ_B을 공격자의 응답값으로 보내야 한다. 비록 공격자가 pw 및 ID_A의 올바른 쌍을 갖고 있어도, 이 값들이 A에 대응하는지 여부는 온라인 공격을 통해서 확인해야 한다. 따라서 A 내부에 온라인 공격에 대응하는 방법을 설정하는 것으로 방어할 수 있다. 온라인 공격이 방어된다면, 공격자는 A가 생성하는 서명 σ_A를 더 이상 받을 수가 없게 된다. 즉 제안된 프로토콜 상에서는 σ_A를 받기 전에 공격자가 정상적인 σ_B를 먼저 제시하는 과정이 선행되어야 하므로, σ_B의 서명 검증이 통과되지 않는 한 세션을 시작하는 제조사라도 더 이상 σ_A를 받을 수 없다.

V. 인증 및 키 교환 프로토콜의 안전성 증명

5.1 외부 공격자에 대한 안전성

정리 1. H_2가 랜덤 오라클로 동작한다고 하자. GQ-IBS가 선택 메시지 공격에 대해 안전하고, f가 유사 난수 함수이고, RSA 모듈러스에서 그룹 위수가 숨겨지고 오라클이 허용되는 강한 디피-헬만(strong DH) 가정이 유효하다면, 제안된 프로토콜은 서명키를 갖지 않는 외부 공격자에 대해 전방향 안전성을 갖는 키 교환 및 사용자 인증을 제공한다.

증명) 전체적인 증명은 [13]을 따른다. 공격자는 (A,B)를 선택하고, ID에 대응하는 서명키 질의를 할 수 있다. Game 0는 실제 게임이고, Game 5는 세션키가 (인증이 성공하면서) 세션과 무관하게 랜덤으로 선택되는 게임이다. 다음의 하이브리드 게임은 Game 1과 Game 5를 공격자가 구분하는 것이 쉽지 않다는 것을 보인다.

Game 0: 실제 게임이다.

Game 1: σ_B가 $g_1,\ \delta$를 포함하는 메시지 $m_B=g_1\|ID_B\|u_A\|u_B\|\delta$와 매칭되지 않으면, 즉 matching conversation이 아니면, 게임을 중단한다. 이 경우는 GQ-IBS의 서명이 위조된 경우이므로, GQ-IBS의 안전성에 환원된다. 그리고 B를 가장한 공격이 성공한 경우이므로, 이 경우를 제외한 이하의 게임에서 B의 인증은 성공한다.

Game 2: H_2 오라클에 $(g^{R_A}, g^{R_B}, g^{R_AR_B})$이 질의되는 경우는 게임을 중단한다. 정당한 디피-헬만 값인지는 strong DH 가정의 오라클로 확인할 수 있다. 이 경우에는 strong DH 가정에 환원된다. 또한 주어진 N의 소인수를 몰라도 H_1 오라클의 출력을 랜덤하게 선택된 r에 대해 r^e로 조작함으로써 모든 ID에 대응하는 서명키를 생성할 수 있음을 상기하자. 이는 공격 대상인 A,B에 대한 서명키를 생성할 수 있다는 것이고, 이 키들이 공격자에게 주어질 수 있다는 것이다. 바로 Game 2부터는 A,B에 대한 서명키가 노출될 수 있다는 것임으로, 전방향 안전성을 의미한다.

Game 3: g_1, K_1, K_2값을 랜덤한 값으로 바꾼다. 이것은 $(g^{R_A}, g^{R_B}, g^{R_AR_B})$이 질의되지 않는 경우, H_2의 출력은 랜덤 오라클의 출력값이므로 Game 2의 분포와 동일하다.

Game 4: σ_A가 $g_1,\ \delta$를 포함하는 메시지 $m_A=g_1\|ID_B\|u_A\|u_B\|\delta\|\sigma_B$와 매칭되지 않으면, 게임을 중단한다. 이 경우도 GQ-IBS의 안전성에 환원된다. 그리고 A를 가장한 공격이 성공한 경우이므로, 이 경우를 제외한 이하의 게임에서 A의 인증은 성공한다.

Game 5: ssk를 랜덤한 w 비트의 값으로 바꾼다. 이 경우는 K_2가 랜덤이므로 유사 난수 함수 f의 안전성에 환원된다.

익명성 증명: 공격자가 (A_1, A_2, B)를 선택하면, 테스트 세션에서 먼저 (A_1, B)로 게임을 진행한다. 그 다음 위 Game 5에 추가적인 게임을 진행하여 (A_2, B)의 실제 게임까지 바꾼다. 이 과정에서 ID, 패스워드의 변환은 K_1이 노출되지 않는 한, A_2의 ID 및 패스워드로 바뀔 수 있다. 이 과정은

유사 난수 함수의 안전성으로 환원된다. 그리고 GQ-IBS 서명 σ_{A_1}는 공격자 관점에서 g_1, δ를 모르기 때문에 지수값 c는 랜덤하게 분포한다. 이 경우 서명 σ_{A_1}는 σ_{A_2}과 비슷한 분포를 가진다. ■

정리 2. *ID*와 *pw*의 엔트로피를 각각 e_{ID}, e_{pw}라 하자. 서명키를 가지고 세션을 시작하는 공격자가 1회 프로토콜 시행에서 인증을 통과할 확률은 $2^{-e_{ID}\times e_{pw}}$이다.

증명) H_2로부터 도출되는 g_1 및 K_1를 알기 때문에 결국 pw 및 ID_A의 전체 경우의 수 중에서 하나를 추측할 확률만큼 인증을 통과할 수 있다. ■

5.2 마스터키를 가진 공격자에 대한 안전성

정리 3. H_2가 랜덤 오라클로 동작한다고 하자. f가 유사 난수 함수이고, RSA 모듈러스에서 그룹 위수가 알려지고 오라클이 허용되는 강한 디피-헬만(strong DH) 가정이 유효하다면, 제안된 프로토콜은 세션을 시작하지 않는, 호기심을 가진 공격자에 대해 전방향 안전성을 갖는 키 교환 및 사용자 인증을 제공한다.

증명) 공격자는 (A, B)를 선택한다. 정리 1과의 차이점은 공격자가 마스터키를 가지고 있으므로 ID에 대응하는 서명키 질의는 생략한다. Game 0는 실제 게임이고, Game 5는 세션키가 (인증이 성공하면서) 세션과 무관하게 랜덤으로 선택되는 게임이다. 다음의 하이브리드 게임은 Game 1과 Game 5를 공격자가 구분하는 것이 쉽지 않다는 것을 보인다.

Game 0: 실제 게임이다.

Game 1: H_2 오라클에 $(g^{R_A}, g^{R_B}, g^{R_AR_B})$이 질의되는 경우는 게임을 중단한다. 정당한 디피-헬만 값인지는 strong DH 가정의 오라클로 확인할 수 있다. 이 경우에는 그룹 위수가 알려진, 즉, N의 소인수가 주어진 strong DH 가정에 환원된다.

Game 2: g_1, K_1, K_2값을 랜덤값으로 바꾼다. 이것은 $(g^{R_A}, g^{R_B}, g^{R_AR_B})$이 질의되지 않는 경우, H_2의 출력은 랜덤 오라클의 출력값이므로 Game 1의 분포와 동일하다.

Game 3: σ_B가 랜덤한 g_1, δ를 포함하는 메시지 $m_B = g_1||ID_B||u_A||u_B||\delta$와 매칭되지 않으면, 게임을 중단한다. 이 경우가 발생할 확률은 GQ-IBS의 해쉬함수 h_1의 출력값 l비트에서 충돌쌍이 발생할 확률보다 작다. 즉, 최대 $(q_{h_1})^2/2^l$보다 작다. 그리고 B를 가장한 공격이 성공한 경우이므로, 이 경우를 제외한 이하의 게임에서 B의 인증은 성공한다.

Game 4: σ_A가 랜덤한 g_1, δ를 포함하는 메시지 $m_A = g_1||ID_B||u_A||u_B||\delta||\sigma_B$와 매칭되지 않으면, 게임을 중단한다. 이 경우도 해쉬함수 h_1의 출력값 l비트에서 충돌쌍이 발생할 확률보다 작다. 그리고 A를 가장한 공격이 성공한 경우이므로, 이 경우를 제외한 이하의 게임에서 A의 인증은 성공한다.

Game 5: ssk를 랜덤한 w 비트의 값으로 바꾼다. 이 경우는 K_2가 랜덤이므로 유사 난수 함수 f의 안전성에 환원된다.

익명성 증명: 공격자가 (A_1, A_2, B)를 선택하면, 테스트 세션에서 먼저 (A_1, B)로 게임을 진행한다. 그 다음 위 Game 5에 추가적인 게임을 진행하여 (A_2, B)의 실제 게임까지 진행한다. 이 과정에서 K_1이 노출되지 않는 한, A_1의 ID 및 패스워드는 A_2의 ID 및 패스워드로 바뀔 수 있다. 이 과정은 유사 난수 함수의 안전성으로 환원된다. 그리고 GQ-IBS 서명에서 지수값 c가 노출되지 않고 랜덤하게 분포하면, (비록 마스터키를 가지는 공격자라 할지라도) 공격자 관점에서 서명 σ_{A_1}는 σ_{A_2}과 비슷한 분포를 가진다. ■

정리 4. (*ID*, *pw*)의 조합으로 이루어지는 엔트로피를 각각 e라 하자. 마스터키와 (*ID*, *pw*)쌍의 집합을 가진, 세션을 시작하는 공격자가 1회 프로토콜 시행에서 인증을 통과할 확률은 2^{-e}이다.

증명) H_2로부터 도출되는 g_1 및 K_1를 알기 때문에 결국 (*ID*, *pw*)쌍의 전체 경우의 수 중에서 하나를 추측할 확률만큼 인증을 통과할 수 있다. ■

VI. 새로운 IP 카메라 동작 프로토콜

이제 제안된 인증 및 키 교환 프로토콜을 이용하

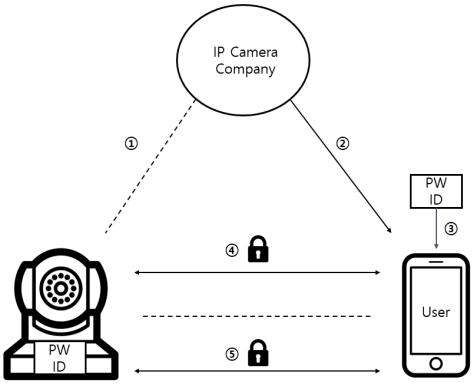

Fig. 3. New IP camera operation protocol

여 전체적인 IP 카메라 동작 프로토콜을 〔그림 3〕으로 설명한다. 먼저 IP 카메라 회사는 IBS 기법을 위한 공개 파라미터(PP) 및 마스터 비밀키(msk)를 생성한다고 하자.

1. IP 카메라 제조사는 각 IP 카메라의 ID에 대응하는 IBS 기반 서명키와 패스워드를 내장하여 제품을 출시한다. 이 경우 ID 및 패스워드는 구매자인 사용자만이 인지할 수 있다고 가정한다.[5)]

2. IP 카메라를 구매한 사용자는 제조사가 지정한 애플리케이션 스토어에서 IP 카메라 구동 소프트웨어를 다운로드한다. 이 경우 소프트웨어에는 임의로 할당된 ID 및 그에 대응하는 IBS 서명키가 탑재된다. 이 과정은 애플리케이션 스토어에서 제공하는 인증서를 이용하여 SSL/TLS와 같은 보안채널 위에서 이루어진다.

3. 사용자가 IP 카메라와 인증 및 키 교환을 시도하는 경우, IP 카메라에서 인지된 ID 및 패스워드를 입력한다.

4. 입력된 ID 및 패스워드를 이용하여 IP 카메라와 사용자는 〔그림 2〕에서 제시된 IBS 기반 인증 및 키 교환 프로토콜을 수행한다. 프로토콜이 정상적으로 수행되면 두 주체는 보안채널을 위한 세션키를 공유한다.

5. 이후의 통신은 세션키를 대칭키로 사용하는 인증 암호 또는 스트림 암호 등을 이용하여 암복호화한다. IP 카메라를 제어하는 메시지 또는 실제 전송되는 동영상 메시지를 암호화하거나, 패스워드를 변경하는 경우에도 사용된다.

5) 현재 IP 카메라는 제품의 하단에 ID 및 초기 패스워드를 부착한다.

VII. 결 론

본 논문에서는 ID-기반 서명기법을 이용하여 IP 카메라 환경에 적합한 인증 및 키 교환 프로토콜을 제시하였다. 제안된 프로토콜은 IP 카메라와 사용자 간 상호 인증 시 IP 카메라에서 제시하는 ID 및 패스워드를 사용자가 입력함으로써 프로토콜 전송 메시지에서 ID 및 패스워드가 노출되지 않도록 설계되었다. 이로 인해 외부 공격자뿐만 아니라 호기심을 갖는 제조사도 해당 IP 카메라의 ID를 특정하는 것이 쉽지 않다. 상호 인증을 위해서는 ID 및 패스워드뿐만 아니라 ID-기반 서명기법을 통한 도전-응답 방식으로 안전성을 강화되었다. 또한 키 교환 프로토콜 수행으로 공유된 세션키는 디피-헬만 방식의 키 교환 방식을 따름으로서 전방향 안전성을 보장한다.

이후의 연구로는 ID 기반 서명보다 더 효율적인, 그래서 IoT 기기에 더욱 적합한 암호기법을 사용해서 사용자 인증 및 키 교환을 완성하는 프로토콜 설계도 의미 있을 것이고, 안전성 모델 측면에서는 제조단계에서부터 악의적인(malicious) 제조사를 공격자로 고려하는 것도 의미가 있을 것이다.

References

〔1〕 J. Park, S. Kim, "Security requirements analysis on IP camera via threat modeling and common criteria," KIPS Transactions on Computer and Communication Systems, 6(3), pp. 121-134, Mar. 2017

〔2〕 A. O'Donnell, "How to secure IP security cameras," https://www.lifewire.com/secure-your-ip-security-cameras-2487488"

〔3〕 I. Badgujar, "How to hack CCTV private cameras," "https//null-byte.wonderhowto.com/forum/hack-cctv-private-cameras-0159437"

〔4〕 J. Eom, M. Seo, J. H. Park, D. H.

Lee, "Efficient ID-based authentication and key exchange protocol," Journal of The Korea Institute of information Security & Cryptology, 26(6), pp. 1387-1399, Dec. 2016

〔5〕 M. Bellare, S. Miner, "A forward secure digital signature scheme," CRYPTO'99, LNCS 1666, pp. 431-448, Aug. 1999

〔6〕 R. Canetti, H. Krawczyk, "Analysis of key exchange protocols and their use for building secure channels," EUROCRYPT'01, LNCS 2045, pp. 453-474, May. 2001

〔7〕 H. Huang, Z. Cao, "An ID-based authenticated key exchange protocol based on bilinear Diffie-Hellman problem," ASIACCS'09, pp. 332-342, Mar. 2009

〔8〕 D. Hofheinz, E. Kiltz, "The group of signed quadratic residues and applications," CRYPTO'09, LNCS 5677, pp. 637-653, Aug. 2009

〔9〕 M. Abdalla, M. Bellare, P. Rogaway, "The oracle Diffie-Hellman assumptions and an analysis of DHIES," CT-RSA'01, LNCS 2020, pp. 143-158, Apr. 2001

〔10〕 L. C. Guillou, J. J. Quisquater, "A paradoxical identity-based signature scheme resulting from zero knowledge," CRYPTO'88, LNCS 403, pp. 216-231, Aug. 1989

〔11〕 M. Bellare, C. Namprempre, G. Neven, "Security proofs for identity-based identification and signature schemes," Journal of Cryptology, 22(1), pp. 1-61, Jan. 2009

〔12〕 D. Galindo, F. D. Garcia, "A Schnorr-like lightweight identity-based signature scheme," AFRICACRYPT'09, LNCS 5580, pp. 135-148, Jan. 2009

〔13〕 H. Krawczyk, H. Wee, "The OPTLS protocol and TLS 1.3," EuroS&P'16, IEEE, Mar. 2016

〈저자소개〉

박 진 영 (Jin Young Park) 학생회원
2018년 2월: 상명대학교 컴퓨터과학과 졸업
〈관심분야〉 인증 및 키 교환, 암호 프로토콜

송 치 호 (Chi-ho Song) 학생회원
2018년 2월: 상명대학교 컴퓨터과학과 졸업
2018년 3월~현재: 상명대학교 컴퓨터과학과 석사과정
〈관심분야〉 인증 및 키 교환, 암호 프로토콜

김 숙 영 (Suk-young Kim) 학생회원
2018년 2월: 상명대학교 컴퓨터과학과 졸업
〈관심분야〉 인증 및 키 교환, 암호 프로토콜

박 주 현 (Ju-hyun Park) 학생회원
2018년 2월: 상명대학교 컴퓨터과학과 졸업
〈관심분야〉 보안프로그래밍

박 종 환 (Jong Hwan Park) 정회원
1999년 2월: 고려대학교 수학과 졸업
2004년 2월: 고려대학교 정보보호대학원 석사
2008년 8월: 고려대학교 정보보호대학원 박사
2013년 9월~현재: 상명대학교 컴퓨터과학과 조교수
〈관심분야〉 함수 암호, 영지식 증명, 암호 프로토콜